November 2009

MONTHLY Cyber Security Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's newsletter provides you with Online Holiday Shopping Tips. 'Tis the Season for Safe Shopping!

Interesting statistic…

Research into this year's holiday shopping patterns from Information Research Inc. predicts that 2009 will be the season of the online budgeter. Only one in five shoppers will not have a budget. In addition, an 18 percent increase in online shopping from 2008 is expected, when only 41 percent of consumers shopped online, according to the firm.

Online Holiday Shopping Tips

The holiday season is approaching quickly and many of us will be shopping online. comScore estimates that in one day alone last year --Cyber Monday on December 1--$846 million was spent in online shopping, marking a 15% jump from 2007. With the increased volume of online shopping, it's important that consumers understand the potential security risks and know how to protect themselves and their information.

Secure Your Computer

Make sure your computer has the latest security updates installed. Check that your anti-virus/anti-spyware software is running and receiving automatic updates. If you haven't already done so, install a firewall before you begin your online shopping.

Upgrade Your Browser

Upgrade your Internet browser to the most recent version available. Review the browser's security settings. Apply the highest level of security available that still gives you the functionality you need.

Ignore Pop-up Messages

Set your browser to block pop-up messages. If you do receive one, click on the "X" at the top right corner of the title bar to close the pop-up message.

Secure Your Transactions

Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the webpage is encrypted. Some browsers can be set to warn the user if they are submitting information that is not encrypted.

2009 Online Shopping Survey…

Despite the economic downturn, e-commerce sales (including event and movie tickets) will grow about 11% to $156.1 billion this year, up from $141.3 billion in 2008, according to the State of Retailing Online 2009. E-commerce sales grew 13% from 2007 to 2008, and online sales will account for 6% of total retail sales this year, up from 5% last year. To retain customers, 53% of online retailers will use e-mails to feature online-only promotions while 55% will use e-mails to either extend invitations to participate in online surveys, highlight new product availability or to gather customer feedback.

Use Strong Passwords

Create strong passwords for online accounts. Use at least eight characters, with numbers, special characters, and upper and lower case letters. Don't use the same passwords for online shopping websites that you use for logging onto your home or work computer. Never share your login and/or password.

Do Not E-mail Sensitive Data

Never e-mail credit card or other financial/sensitive information. E-mail is like sending a postcard and other people have the potential to read it.

Do Not Use Public Computers or Public Wireless to Conduct Transactions

Don't use public computers or public wireless for your online shopping. Public computers may contain malicious software that steals your credit card information when you place your order. Criminals may be monitoring public wireless for credit card numbers and other confidential information.

Review Privacy Policies

Review the privacy policy for the website/merchant you are visiting. Know what information the merchant is collecting about you, how it will be used, and if it will be shared or sold to others.

Make Payments Securely

Pay by credit card rather than debit card. Credit/charge card transactions are protected by the Fair Credit Billing Act. Cardholders are typically only liable for the first $50 in unauthorized charges. If online criminals obtain your debit card information they have the potential to empty your bank account.

Use Temporary Account Authorizations

Some credit card companies offer virtual or temporary credit card numbers. This service gives you a temporary account number for online transactions. These numbers are issued for a short period of time and cannot be used after that period.

Select Merchants Carefully

Limit your online shopping to merchants you know and trust. Confirm the online seller's physical address and phone number in case you have questions or problems. If you have questions about a merchant, check with the Better Business Bureau or the Federal Trade Commission.

Keep Records

Keep a record of your online transactions, including the product description and price, the online receipt, and copies of every e-mail you send or receive from the seller. Review your credit card and bank statements for unauthorized charges.

this newsletter is brought to you by…

MS-ISAC

www.msisac.org

www.its.ms.gov/services_security.shtml

What to do if you encounter problems with an online shopping site:

If you have problems shopping online, contact the seller or site operator directly. If those attempts are not successful, you may wish to contact the following entities:

- the Attorney General's office in your state
- your county or state consumer protection agency
- the Better Business Bureau at: www.bbb.org
- the Federal Trade Commission at: www.ftc.gov/

For more information on securing mobile communication devices, please visit:

- **US-CERT:** www.us-cert.gov/cas/tips/ST07-001.html
- **National Cyber Security Alliance:** www.staysafeonline.org/content/online-shopping
- **OnGuard Online**: www.onguardonline.gov/topics/online-shopping.aspx
- **Online Cyber Safety:** www.bsacybersafety.com/video/
- **Microsoft:** www.microsoft.com/protect/fraud/finances/shopping_us.aspx

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to redistribute this newsletter in whole for educational, non-commercial purposes.